Target CI v1.5

GUIDE DE CYBERSÉCURITÉ

Français

Mise à jour : septembre 2025

Une marque Sonova

Sommaire

1. INTRODUCTION

Ce document fournit des informations techniques de sécurité et de confidentialité sur le système logiciel Target CI v1.5 d'Advanced Bionics, ci-après « logiciel d'appareillage ». Le logiciel d'appareillage est conçu pour être utilisé par des audioprothésistes qualifiés pour configurer (c'est-à-dire appareiller) des appareils auditifs pour les patients ayant reçu des implants cochléaires d'Advanced Bionics.

Ce document se concentre spécifiquement sur les considérations de cybersécurité et de confidentialité qui sont pertinentes pour l'utilisation du logiciel d'appareillage. Il comprend une évaluation des contrôles de sécurité et de confidentialité actuellement intégrés au logiciel, ainsi que ceux qui devraient être appliqués et configurés dans l'environnement informatique où le produit sera utilisé aux fins prévues.

Ce document ne fournit pas d'informations techniques de sécurité et de confidentialité sur :

- les versions précédentes du logiciel d'appareillage AB
- tout logiciel AB autre que Target CI v1.5
- les sites Web AB
- les applications mobiles AB
- les appareils auditifs AB

1.1 ABRÉVIATIONS ET DÉFINITIONS :

Acronyme	Terme
FSW	Logiciel d'appareillage
HCP	Audioprothésiste
SaMD	Le logiciel en tant que dispositif médical
AB	Advanced Bionics
IFU	Instructions d'utilisation

2. AUTRES RESSOURCES

2.1 SERVICE CLIENT

Pour les personnes situées aux États-Unis et au Canada, Advanced Bionics offre un numéro de téléphone d'assistance technique sans frais (877-271-6727) assurant une assistance professionnelle dédiée du lundi au vendredi de 5 h à 17 h, heure du Pacifique.

Pour les personnes situées en dehors des États-Unis et du Canada, une assistance technique est disponible au niveau régional. Pour toute question relative au logiciel d'appareillage ou en cas de problème de matériel ou de programmation, veuillez contacter votre représentant AB local.

2.2 AB PRO PORTAL

Le logiciel d'appareillage et la documentation associée peuvent être téléchargés sur https://www.abproportal.com ou sur Sonova Web Client. Une connexion à un compte est requise. Cette ressource peut ne pas être disponible sur tous les marchés ; contactez votre représentant AB pour plus d'informations.

2.3 GUIDE D'INSTALLATION AVANCÉ

Le guide d'installation avancé de Target CI v1.5 est disponible sur demande. Le guide fournit des informations techniques sur le programme d'installation du logiciel d'appareillage, y compris les options de ligne de commande pour les installations silencieuses et automatisées.

2.4 MDS2

La déclaration du fabricant sur la sécurité des dispositifs médicaux (MDS2) est un formulaire standard de l'industrie contenant des réponses sur la sécurité et la confidentialité concernant le logiciel d'appareillage d'AB. Le formulaire est disponible sur demande.

2.5 INSTRUCTIONS D'UTILISATION

Les instructions d'utilisation sont fournies avec le support d'installation du logiciel. Pour certains marchés, les instructions d'utilisation électroniques sont disponibles pour le téléchargement à l'adresse www.advancedbionics.com/ifu

Les sections suivantes des instructions d'utilisation peuvent être pertinentes pour les professionnels de l'informatique :

- Description du produit
- Configuration minimale requise et caractéristiques de performance
- Consignes pour la sécurité informatique
- Instructions d'installation
- Assistance technique

2.6 HIMSA

HIMSA est un fournisseur de logiciels tiers qui produit Noah System 4, un système logiciel conçu pour le secteur des soins auditifs qui fournit aux audioprothésistes un système indépendant des fournisseurs pour effectuer des tâches liées aux clients.

Le logiciel d'appareillage peut éventuellement être configuré pour utiliser Noah System 4 pour le stockage des données plutôt qu'une base de données locale.

La page Web de sécurité de HIMSA fournit des réponses aux questions courantes sur la sécurité informatique concernant Noah System 4.

https://www.himsa.com/support/noah-enterprise-support/security-questionnaire-support/

https://www.himsa.com/support/noah-enterprise-support/security-considerations/

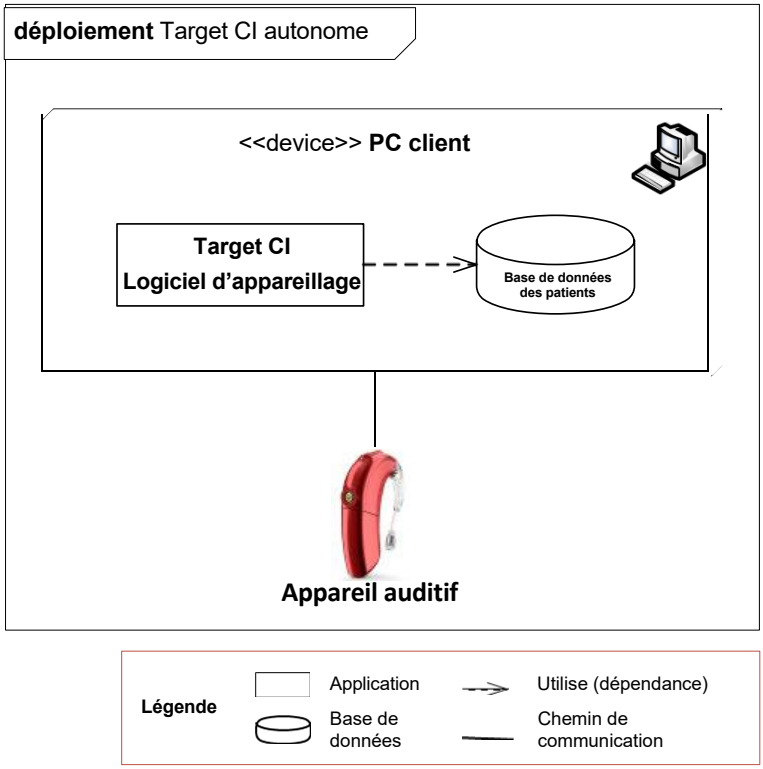
Consultez la section Sécurité du Centre d'apprentissage de HIMSA pour obtenir des informations de sécurité supplémentaires : https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

3. DIAGRAMMES DE RÉSEAU ET DE CONTEXTE

Il existe deux modèles de déploiement pris en charge pour le logiciel d'appareillage, qui est une application client (SaMD) installée sur un ordinateur Microsoft Windows de bureau disponible dans le commerce. Le logiciel n'inclut aucun matériel ni système d'exploitation.

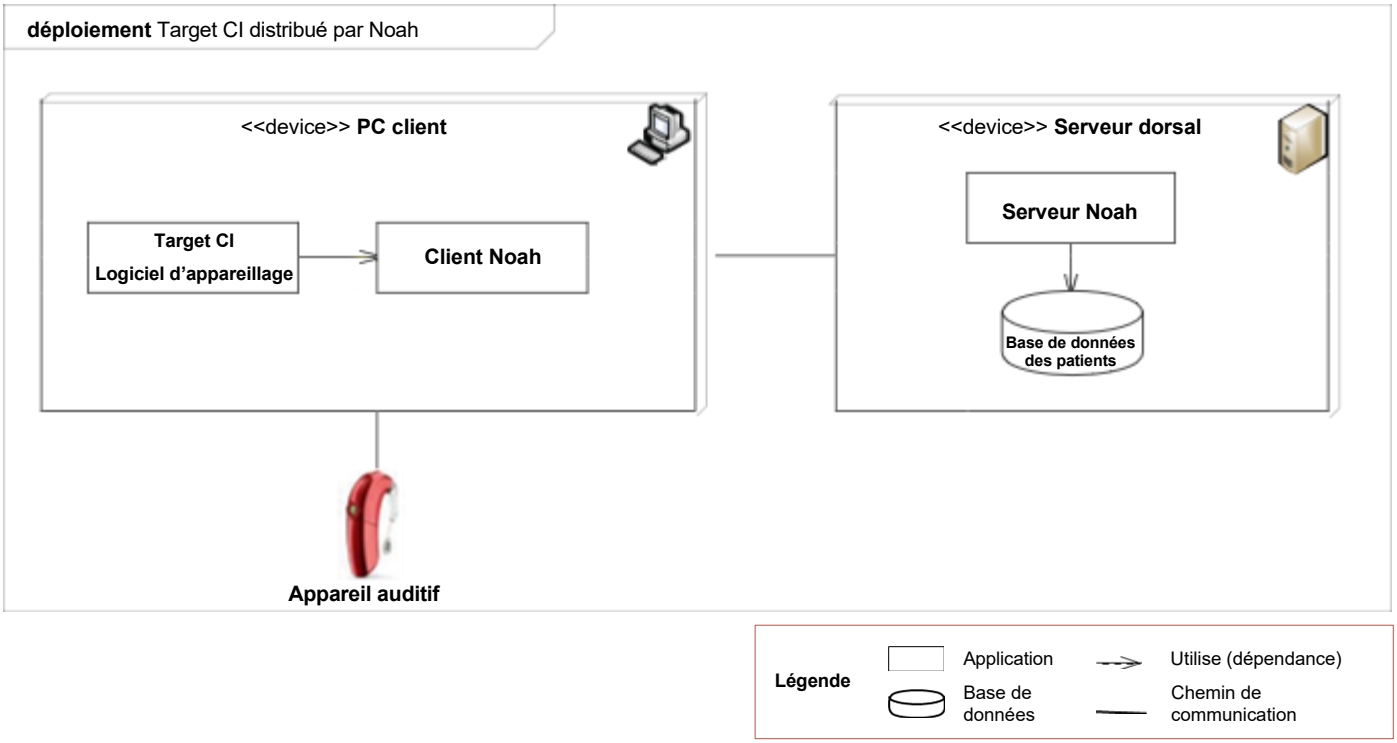
3.1 MODÈLE DE DÉPLOIEMENT 1 : AUTONOME

Dans le modèle de déploiement autonome, le logiciel d'appareillage est déployé sur un ordinateur de bureau client. La base de données des patients est stockée sur le même ordinateur de bureau et installée avec le logiciel d'appareillage.



3.2 MODÈLE DE DÉPLOIEMENT 2 : DISTRIBUÉ PAR NOAH

Dans le modèle de déploiement distribué par Noah, le logiciel d'appareillage est déployé sur un ou plusieurs PC clients. Noah, un système de gestion tiers des patients, est déployé sur un serveur interne accessible aux PC clients. La base de données des patients est stockée sur le serveur Noah et accessible via le réseau par un ou plusieurs PC clients.

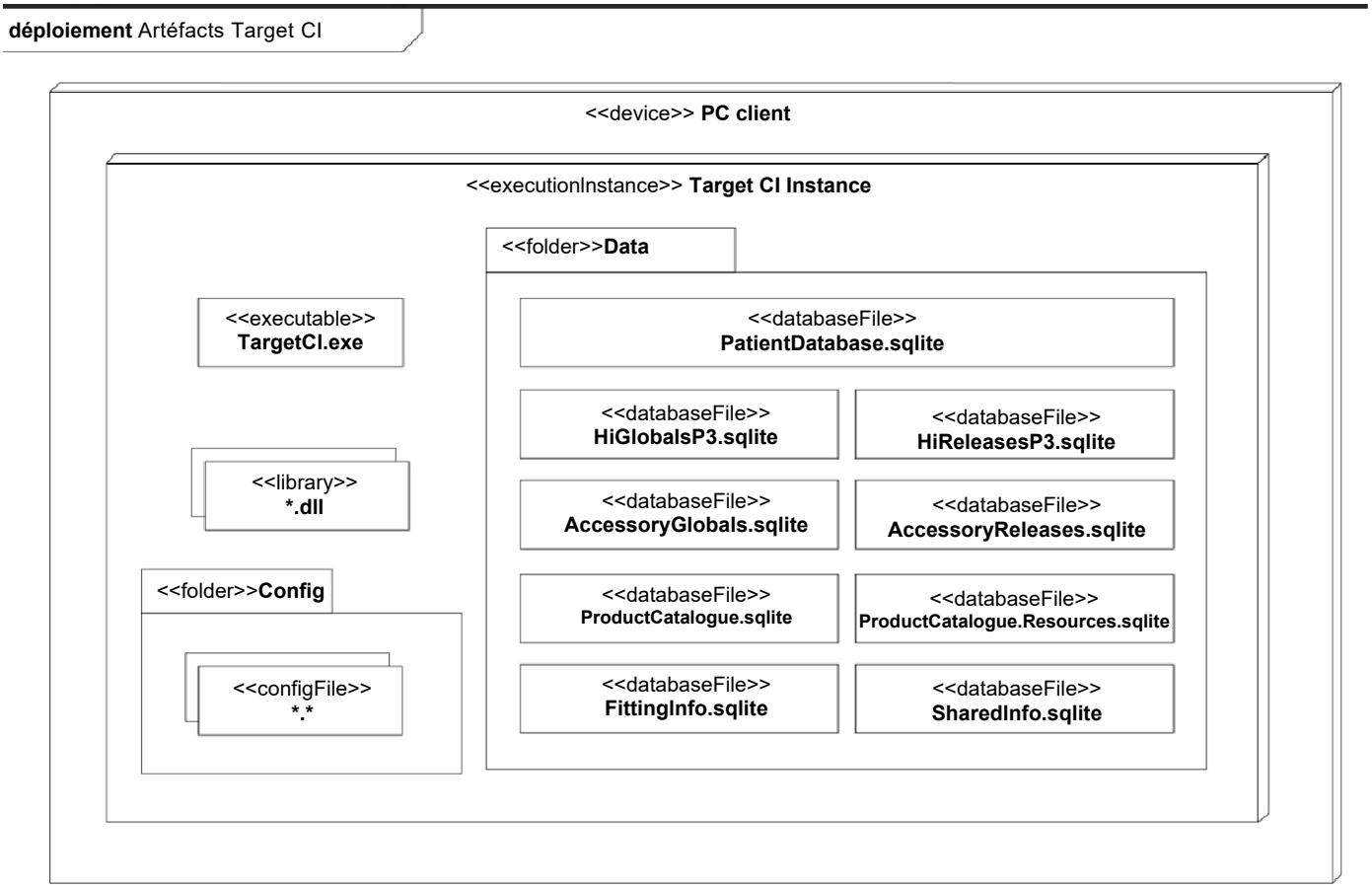


3.3 ARTÉFACTS DE DÉPLOIEMENT

Le logiciel d'appareillage s'installe avec un fichier exécutable et un ensemble de fichiers associés comprenant des DLL de composants, des fichiers de configuration et des fichiers de base de données SQLite. Les fichiers de configuration sont installés dans le dossier « %ProgramData%\ Advanced Bionics\Target CI\Target CI\Config » et les fichiers de base de données sont installés dans le dossier « %ProgramData%\Advanced Bionics\Target CI\Target CI\Data ». Le dossier Data contient un seul fichier de base de données transactionnelle et plusieurs fichiers de base de données d'informations.

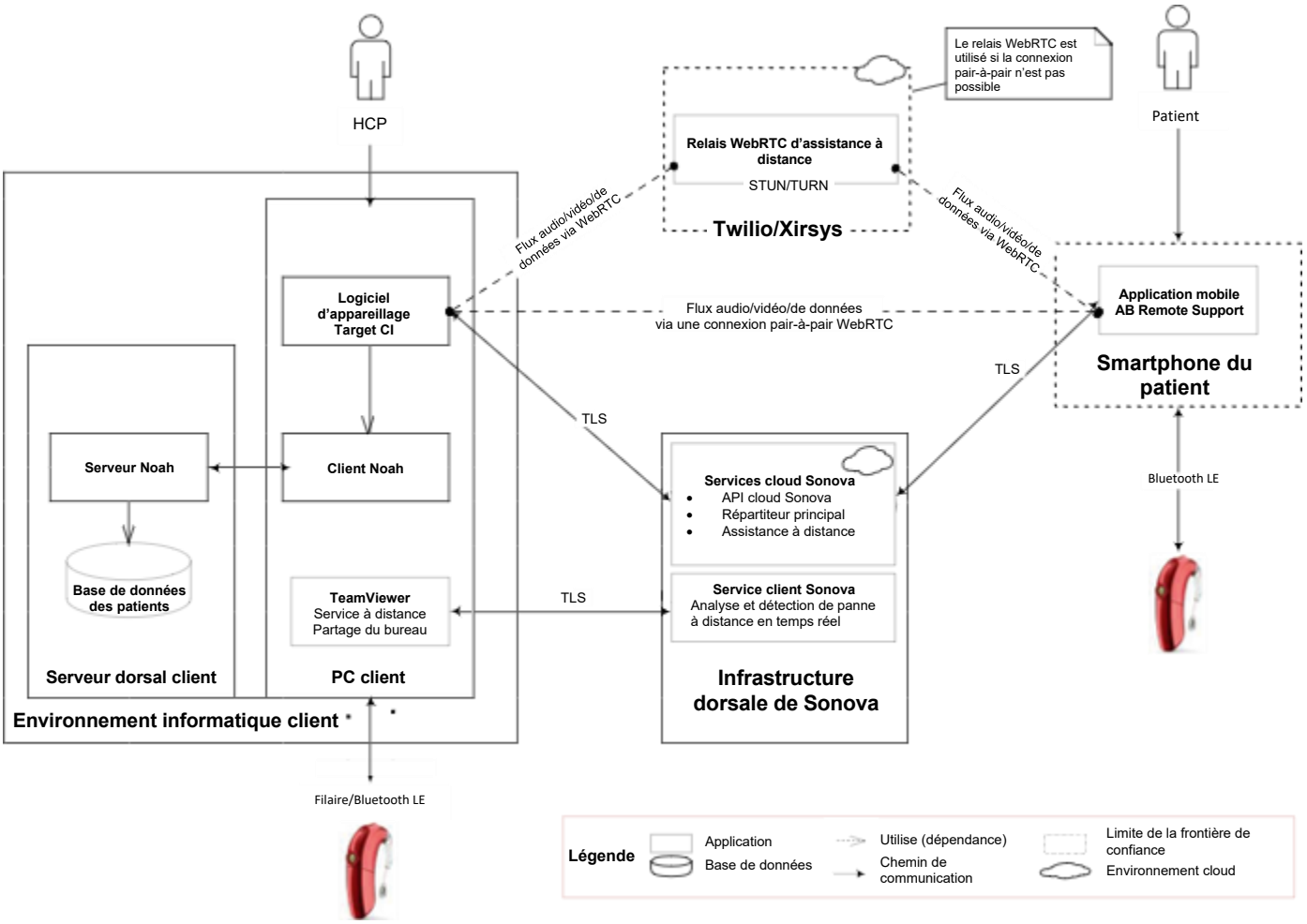
La base de données transactionnelle, PatientDatabase.sqlite, stocke les données démographiques et d'appareillage du patient et n'est installée que lorsque le logiciel d'appareillage est déployé en mode autonome.

Lorsque le logiciel d'appareillage est déployé en tant que module Noah, le système Noah fournit les services de persistance des données des patients requis au logiciel d'appareillage. Les fichiers sqlite restants font partie intégrante du logiciel d'appareillage et sont requis pour tous les modèles de déploiement.



3.4 INTERCONNEXIONS DU SYSTÈME

Le diagramme et le tableau ci-dessous illustrent les principales interconnexions du système. En règle générale, seule une partie des interconnexions disponibles est utilisée.



Source/ Destination	Service	Protocole	Port	Description
Appareils auditifs	Communication des appareils auditifs	Connexion filaire / Bluetooth® Low Energy	N/A	Utilisée pour communiquer avec les appareils auditifs à des fins de contrôle, de configuration et de lecture des données et de l'état
Noah	Module API Noah 4	.NET Remoting	N/A	Interface principale du module utilisée pour accéder au logiciel Noah (dans le modèle de déploiement distribué de Noah uniquement)

Source/ Destination	Service	Protocole	Port	Description
Services cloud Sonova	API cloud Sonova, répartiteur principal, assistance à distance	SOAP, REST	443	Les services Sonova hébergés dans un centre de données Microsoft Azure sont utilisés pour : • récupérer les données de configuration du client du logiciel d'appareillage à partir du stockage dorsal de Sonova • transférer des données de journalisation et d'analyse • mettre en place des sessions d'appareillage à distance en temps réel
Twilio/Xirsys, application mobile AB Remote Support	Assistance à distance	WebRTC	Liste des ports disponible sur demande	Les services de communication cloud de Twilio sont hébergés sur des plateformes cloud tierces, notamment Amazon Web Services (AWS) et Google Cloud Platform (GCP). Ces services sont utilisés exclusivement par la fonctionnalité d'assistance à distance du logiciel d'appareillage, qui permet la signalisation WebRTC et les sessions d'appareillage à distance en temps réel.
Service client AB	Partage du bureau	Protocole propriétaire TeamViewer	5938, 443, 80 Reportez-vous à TeamViewerPorts	Utilisé pour effectuer une analyse et une détection de panne à distance en temps réel des problèmes affectant les installations de logiciels d'appareillage. Reportez-vous à la section 6.6 SERVICE À DISTANCE pour plus d'informations.

4. CONFIGURATION REQUISE

Système d'exploitation	Windows 10, Professionnel/Entreprise, 64 bits
.NET Framework	Version 4.8
Processeur	Intel® Core™ i5 ou équivalent avec des performances égales ou supérieures
RAM	4 Go ou plus
Espace sur le disque dur	3 Go ou plus
Configuration minimale requise pour l'affichage	• Résolution 1280 x 1024 (mise à l'échelle maximale 125 %) • Couleur 24 bits
Pilotes de périphériques	• Pilote Noahlink Wireless (la dernière version disponible auprès de HIMSA est requise si vous utilisez une interface tierce de programmation Noahlink Wireless connectée par USB). • Pilote CPI-3 (requis si vous utilisez une interface de programmation CPI-3 connectée par USB).
Base de données	SQLite ou Noah System 4 (version 4.14 ou supérieure)
Connexion Internet	Connexion Internet requise pour l'assistance à distance et la journalisation de l'analyse, reportez-vous à la section 4.4 Interconnexions du système ; intranet requis lors de l'utilisation de Noah System 4 en réseau.
Ports réseau	Voir la section 3.4 Interconnexions du système ; voir la section 3. Autres ressources — HIMSA pour les ports utilisés par Noah System 4.

5. INSTALLATION

5.1 EXIGENCES

Un compte administrateur est requis pour installer le logiciel d'appareillage. Une fois le logiciel installé, il peut être exécuté sans autorisations administratives ou de haut niveau.

Consultez la section 8. Intégrité du logiciel, pour obtenir des informations sur la validation de l'intégrité du logiciel avant l'installation.

Avant l'installation, il est recommandé aux administrateurs du système de s'assurer que :

• la version du logiciel d'appareillage à installer est la dernière disponible ;

• le système d'exploitation sous-jacent est à jour.

5.2 TYPES DE PROGRAMMES D'INSTALLATION

Deux programmes d'installation sont disponibles pour installer le logiciel d'appareillage :

• Programme d'installation standard

• Programme d'installation informatique professionnelle

Le programme d'installation informatique professionnelle est un fichier MSI unique et exclut les composants prérequis, mais est par ailleurs équivalent au programme d'installation standard.

Les composants prérequis incluent Microsoft .NET Framework v4.8 et les packages Microsoft Visual Studio C++ Redistibutable.

Les deux programmes d'installation prennent en charge les scénarios d'installation avancés, y compris l'installation silencieuse.

Le programme d'installation informatique professionnelle ne doit être utilisé que si votre organisation exige que les composants prérequis soient installés et gérés par votre organisation et non par le programme d'installation du logiciel d'appareillage. Dans tous les autres cas, le programme d'installation standard doit être utilisé.

Le programme d'installation informatique professionnelle peut être obtenu auprès du représentant clinique AB. Le programme d'installation informatique professionnelle ne peut pas être utilisé pour réparer, réinstaller ou désinstaller des installations effectuées par le programme d'installation standard. Le programme d'installation standard ne peut pas être utilisé pour réparer, réinstaller ou désinstaller des installations effectuées par le programme d'installation informatique professionnelle.

6. CONTRÔLES DE SÉCURITÉ

Le logiciel d'appareillage est une application client installée sur un ordinateur de bureau Microsoft Windows disponible dans le commerce. Le logiciel d'appareillage peut être installé en tant qu'application autonome ou en tant que module Noah.

6.1 AUTHENTIFICATION – DÉPLOIEMENT AUTONOME

Lorsque le logiciel d'appareillage est installé en tant qu'application autonome, il s'appuie sur les mécanismes de contrôle d'accès fournis par le système d'exploitation hôte. Le système d'exploitation hôte peut être configuré par le personnel informatique du client pour gérer l'authentification. Le logiciel d'appareillage ne dispose pas d'une telle fonctionnalité intégrée. Advanced Bionics recommande à chaque utilisateur de se connecter au système d'exploitation hôte avec un compte utilisateur unique.

6.2 AUTHENTIFICATION – DÉPLOIEMENT DE NOAH

Lorsque le logiciel d'appareillage est installé en tant que module Noah, le contrôle d'accès est assuré par Noah System 4. Consultez www.HIMSA.com pour connaître les contrôles d'audit utilisés par Noah System 4.

6.3 AUTORISATION

Le logiciel d'appareillage ne restreint pas l'accès à ses fonctionnalités en fonction des rôles des utilisateurs individuels. Le logiciel prend en charge une seule fonction principale d'appareillage des appareils auditifs du patient et un seul rôle de professionnel de l'appareillage. Les contrôles d'accès basés sur les rôles ne sont pas applicables.

6.4 AUDIT – DÉPLOIEMENT AUTONOME

Lorsque le logiciel d'appareillage est installé en tant qu'application autonome, il s'appuie sur les mécanismes d'audit fournis par le système d'exploitation hôte. Le logiciel d'appareillage ne dispose pas d'une telle fonctionnalité intégrée. Le système d'exploitation hôte peut être configuré par le personnel informatique du client pour enregistrer les lancements/exécutions du logiciel d'appareillage et les identifiants des utilisateurs. Advanced Bionics recommande à chaque utilisateur de se connecter au système d'exploitation hôte avec un compte utilisateur unique pour faciliter l'audit.

6.5 AUDIT – DÉPLOIEMENT DE NOAH

Lorsque le logiciel d'appareillage est installé en tant que module Noah, les journaux d'audit sont fournis par le système Noah. Consultez https://www.himsa.com/ pour connaître les contrôles d'audit utilisés par Noah System 4.

6.6 ACCÈS À DISTANCE

La fonctionnalité de partage de bureau permet une analyse et une détection de panne à distance en temps réel des problèmes affectant les installations de logiciels d'appareillage. Cette fonctionnalité est basée sur l'outil tiers TeamViewer QuickSupport (déployé par défaut avec le logiciel d'appareillage) et permet aux professionnels du service client AB de se connecter à distance à l'ordinateur de l'audioprothésiste et d'obtenir un contrôle total sur le bureau, y compris l'accès au système d'exploitation et de fichiers sous-jacent.

Pour établir une session de partage du bureau, l'interaction de l'audioprothésiste est requise. L'audioprothésiste doit d'abord exécuter l'outil TeamViewer QuickSupport (par exemple, via le logiciel d'appareillage Target CI) et communiquer ses informations d'identification TeamViewer à l'équipe d'Assistance AB via un canal de communication hors bande (par exemple, un appel téléphonique).

Le nom du membre de l'équipe d'Assistance AB et son identifiant TeamViewer sont affichés par défaut sur l'écran de l'ordinateur de l'audioprothésiste pendant chaque session de partage du bureau active.

Tout le trafic réseau de partage du bureau est sécurisé et respecte ou dépasse les normes des protocoles et algorithmes cryptographiques (échange de clés publiques/privées RSA et chiffrement de session AES 256 bits).

TeamViewer QuickSupport peut être supprimé manuellement sans affecter les autres fonctionnalités du FSW Target. Le programme d'installation du FSW Target prend en charge un paramètre d'installation de ligne de commande pour permettre une installation de ligne de commande du FSW Target sans inclure l'outil TeamViewer QuickSupport.

7. PROTECTION DES INFORMATIONS

7.1 POLITIQUE DE CONFIDENTIALITÉ D'ADVANCED BIONICS

La politique de confidentialité décrivant comment Advanced Bionics collecte, transfère, stocke et utilise les données personnelles peut être téléchargée sur : AdvancedBionics.com/privacy.

Advanced Bionics n'héberge, ne stocke, ne sauvegarde et n'a accès à aucune donnée stockée dans le logiciel d'appareillage ou dans les bases de données Noah, à moins que les données ne soient expressément envoyées à Advanced Bionics.

7.2 NORMES FÉDÉRALES DE TRAITEMENT DE L'INFORMATION (FIPS)

Target CI v1.5 est conforme aux normes de chiffrement FIPS 140-2.

7.3 SÉCURITÉ DES DONNÉES EN TRANSIT

La sécurité des communications est assurée et activée dans toutes les communications réseau entrantes et sortantes du logiciel d'appareillage. À l'exception de la fonctionnalité d'assistance à distance (qui utilise le protocole WebRTC) et de la communication Bluetooth avec les appareils auditifs et les accessoires, toutes les autres connexions sont protégées par le protocole Transport Layer Security (TLS) qui assure la confidentialité, l'intégrité et l'authenticité.

TLS

La configuration TLS est conforme aux bonnes pratiques et aux recommandations de sécurité actuelles documentées dans le document BCP 195 – Recommandations pour une utilisation sécurisée de TLS et DTLS, BCP195, notamment :

- Ne prend pas en charge les versions de SSL et TLS antérieures à 1.2
- Ne prend pas en charge les suites de chiffrement qui utilisent des algorithmes cryptographiques offrant moins de 128 bits de sécurité

- Prend en charge les extensions TLS recommandées du BCP 195
- Ne prend pas en charge les extensions non sécurisées du BCP 195

DTLS

Le chiffrement est une fonctionnalité obligatoire de WebRTC et est appliqué à tous les flux multimédias envoyés via WebRTC. Le protocole de chiffrement utilisé dépend du type de canal ; les flux de données sont chiffrés à l'aide de DTLS et les flux multimédias sont chiffrés à l'aide du protocole SRTP (Secure Real-time Transport Protocol) utilisé, car il s'agit d'une option plus légère que DTLS.

Consultez le lien suivant pour obtenir des informations plus détaillées sur la configuration de sécurité de l'assistance à distance WebRTC :

https://developer.liveswitch.io/liveswitch-server/server/security.html

BLE

La communication sans fil Bluetooth Low Energy avec les appareils auditifs et les accessoires est chiffrée et protégée en intégrité par défaut (sauf pour les cas d'utilisation d'identification et de détection). De plus, la durée du mode d'appairage Bluetooth de l'appareil auditif est limitée dans le temps. Reportez-vous à la documentation disponible sur l'appareil auditif pour une description plus détaillée de la sécurité du canal de communication Bluetooth.

7.4 SÉCURITÉ AU REPOS

Base de données des patients – Modèle de déploiement autonome

Si le logiciel d'appareillage est installé en tant qu'application autonome, la base de données des patients est stockée localement à l'adresse : C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

Ces dossiers ne sont pas chiffrés au repos par défaut. Les informations de santé protégées (ISP) et les informations personnelles identifiables (IPI) sont stockées dans une base de données interne au logiciel d'appareillage et ne sont pas transmises sur le réseau.

Dans certaines juridictions, la réglementation peut exiger le chiffrement de toutes les données des patients afin d'éviter toute responsabilité potentielle en cas de perte ou de vol de données. Activez BitLocker ou un chiffrement complet du disque équivalent (au niveau du système d'exploitation ou basé sur le matériel) pour protéger les données contre tout accès ou copie non autorisés pendant que les données sont au repos.

BitLocker est une fonctionnalité Windows intégrée qui chiffre l'intégralité du disque et nécessite une authentification pour y accéder. Consultez toujours les directives officielles de Microsoft et la politique de sécurité informatique de votre organisation avant d'activer BitLocker.

Comment activer BitLocker

Des droits d'administration sont requis pour gérer BitLocker.

1. Rechercher « Gérer BitLocker »

   Ouvrez le menu Démarrer, saisissez « Gérer BitLocker » et sélectionnez-le dans les résultats de la recherche.

2. Sélectionner le disque système

   Choisissez le disque sur lequel Windows est installé pour configurer les paramètres de chiffrement.

3. Choisir une méthode de déverrouillage

   Sélectionnez l'une des options suivantes :

   –TPM uniquement

   –TPM + PIN

   –TPM + clé USB

   Suivez les bonnes pratiques de Microsoft et la politique de sécurité informatique de votre organisation lors de la sélection de la méthode de déverrouillage.

4. Sauvegarder la clé de récupération

   Sauvegardez la clé de récupération à l'aide de méthodes sécurisées et approuvées par l'entreprise. Les options recommandées incluent :

   –le stockage dans Microsoft Entra ID (anciennement Azure AD) ou Active Directory pour les appareils appartenant au domaine ;

   –l'enregistrement dans un emplacement réseau sécurisé et à accès contrôlé avec chiffrement et journalisation d'audit ;

   –l'utilisation d'une solution d'entiercement de clés gérée approuvée par votre organisation.

   Évitez d'enregistrer la clé sur des disques locaux, des clés USB ou de l'imprimer, sauf si cela est explicitement autorisé par la politique. Les clés de récupération doivent être protégées avec la même rigueur que les autres informations d'identification sensibles et immédiatement renouvelées si elles sont exposées.

5. Démarrer le chiffrement

   Choisissez :

   –Disque entier : recommandé pour la plupart des scénarios d'entreprise. Chiffre tous les secteurs, y compris l'espace inutilisé, pour empêcher la rémanence des données.

Base de données des patients – Module de déploiement distribué de Noah

Lorsque le logiciel d'appareillage est installé en tant que module Noah, les informations personnelles identifiables sont stockées dans la base de données des patients hébergée par Noah. La base de données des patients hébergée par Noah peut se trouver sur une autre machine. Les informations personnelles identifiables et autres données des patients sont conservées par le logiciel Noah et le chiffrement des données au repos des patients est assuré par le système Noah. Le logiciel d'appareillage peut transmettre/recevoir les informations personnelles identifiables via une connexion réseau filaire ou sans fil lorsqu'une base de données Noah est configurée pour l'accès au réseau.

Les informations personnelles identifiables stockées dans la base de données Noah en réseau seront visibles par d'autres utilisateurs d'appareils sur différents PC disposant d'autorisations sur la même base de données en réseau. La base de données Noah peut également être configurée pour un accès hors réseau et installée sur le même PC que le logiciel d'appareillage.

Noah empêche le logiciel d'appareillage d'accéder à la base de données des dossiers des patients. Lorsqu'un utilisateur ouvre un dossier patient dans le logiciel d'appareillage via Noah Client, le logiciel d'appareillage ne peut que lire et écrire dans le dossier patient actuellement ouvert et n'est pas en mesure d'accéder aux autres dossiers patients dans la base de données Noah.

Consultez la section www.HIMSA.com pour connaître les normes de chiffrement utilisées par Noah System 4.

Fichiers d'exportation de RMA

Le logiciel d'appareillage permet d'exporter les informations client vers un fichier. Le fichier RMA peut être envoyé à Advanced Bionics pour résoudre les problèmes de RMA ou d'assistance associés.

Le fichier RMA est chiffré de manière asymétrique avec RSA à l'aide d'une longueur de clé de 512 bits. Le logiciel d'appareillage ne dispose d'aucune fonctionnalité permettant de déchiffrer un fichier RMA.

Fichiers d'exportation anonymisés

Le logiciel d'appareillage permet d'exporter les informations client vers un fichier anonymisé. Les informations personnelles identifiables du client, telles que la date de naissance et le nom, sont remplacées par des valeurs génériques. Le fichier n'est pas chiffré et peut être importé dans la même instance ou dans une instance différente du logiciel d'appareillage.

Fichiers d'exportation standard

Le logiciel d'appareillage permet d'exporter les informations client vers un fichier d'exportation standard. Le fichier utilise un format binaire propriétaire et n'est pas chiffré. Le fichier peut être importé dans la même instance ou dans une instance différente du logiciel d'appareillage. Lors de l'utilisation de cette fonctionnalité, les utilisateurs de logiciels d'appareillage doivent s'assurer que les fichiers d'exportation standard sont traités conformément à leurs politiques informatiques locales pour la gestion des informations personnelles identifiables non chiffrées.

Appareil auditif

Le logiciel d'appareillage stocke les informations client sur l'appareil auditif du client. Les informations personnelles identifiables, telles que le nom et la date de naissance du client, ne sont pas stockées sur l'appareil auditif. Les autres informations non IPI sont stockées à l'aide du chiffrement PBKDF2 avec une clé de 128 bits.

Le logiciel d'appareillage peut transmettre/recevoir des informations client non-IPI depuis/vers un appareil auditif via un appareil filaire propriétaire (c.-à-d. CPI-3), l'application mobile AB Remote Support ou un appareil Noahlink Wireless. L'appareil Noahlink Wireless se connecte à l'appareil auditif à l'aide de Bluetooth Low Energy (BLE) via un canal chiffré AES de 128 bits BLE standard.

8. INTÉGRITÉ DU LOGICIEL

8.1 VÉRIFICATION DU SUPPORT D'INSTALLATION TÉLÉCHARGÉ

Le support d'installation du logiciel d'appareillage Target CI peut être téléchargé dans certaines régions depuis Pro Portal d'Advanced Bionics ou Sonova Web Client. Le support d'installation téléchargé peut être authentifié à l'aide de n'importe quel outil de hachage SHA-256 de confiance.

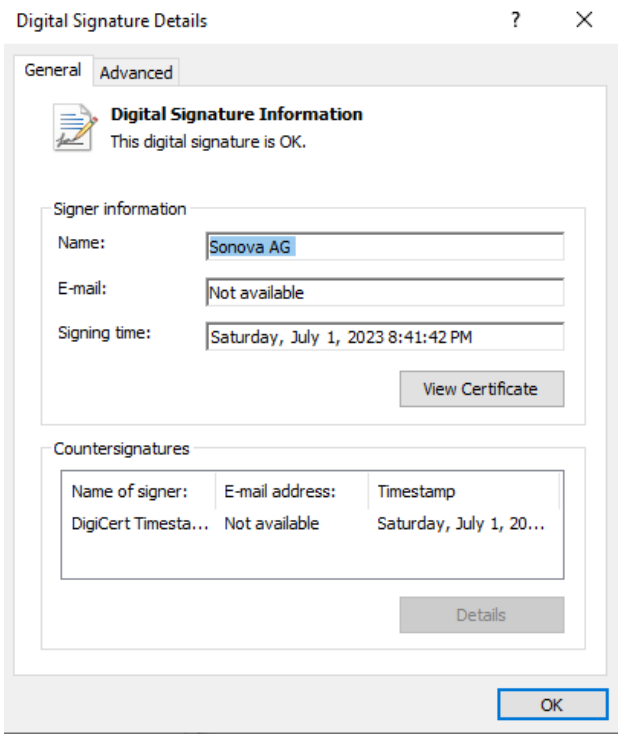
Le hachage SHA256 du fichier zip d'installation standard est :
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

Le hachage SHA256 du fichier zip d'installation pour professionnels de l'informatique est :
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 VÉRIFICATION MANUELLE DU LOGICIEL D'APPAREILLAGE AVANT L'INSTALLATION

Les utilisateurs peuvent effectuer les étapes suivantes pour vérifier l'intégrité et l'authenticité du logiciel d'appareillage avant l'installation :

1. Ouvrez l'Explorateur Windows et accédez au dossier racine du support d'installation du logiciel d'appareillage. Si votre support d'installation est une clé USB, insérez-la dans un port USB et accédez à sa racine. Si votre support d'installation est un fichier zip, décompressez-le dans un dossier et accédez à ce dossier.
2. Faites un clic droit sur SonovaVerify.exe et sélectionnez Propriétés dans le menu contextuel.
3. Sélectionnez l'onglet Signatures numériques.
4. Double-cliquez sur la signature SHA256 « Sonova AG ».
5. Vérifiez que les éléments de la signature sont valides. Vérifiez en particulier que le message « The digital signature is OK. » (La signature numérique est valide.) apparaît en haut et que le nom du signataire et l'heure de signature correspondent à l'image suivante :



1. Fermez les boîtes de dialogue contextuelles et double-cliquez sur SonovaVerify.exe.
2. Vérifiez que « NO ERRORS DETECTED » (AUCUNE ERREUR DÉTECTÉE) s'affiche comme indiqué dans l'image suivante :

L'image montre que SonovaVerify a authentifié et vérifié les signatures numériques de tous les fichiers sur le support d'installation, y compris le programme d'installation. Cela permet de vérifier que le support d'installation n'a pas été altéré, corrompu ou compromis d'une autre manière. SonovaVerify affichera des avertissements ou des messages d'erreur si des fichiers ou des dossiers sont manquants ou si des fichiers ou des dossiers inattendus ont été ajoutés au support d'installation.

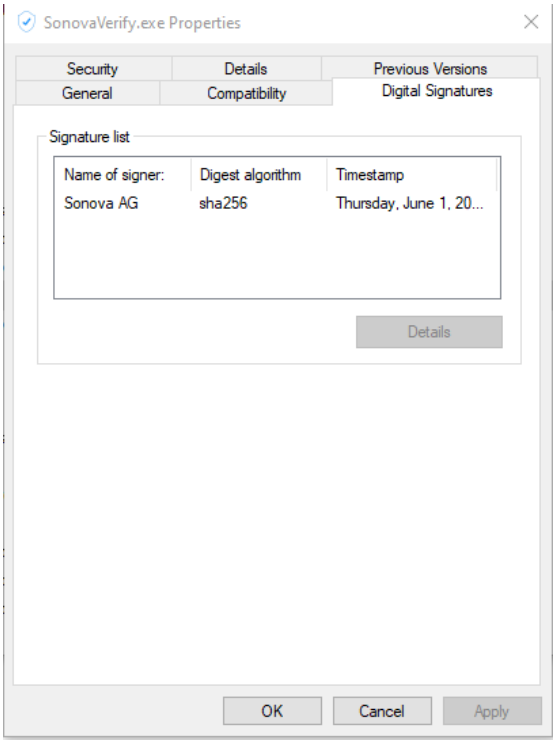
8.3 VÉRIFICATION AUTOMATIQUE DE L'INTÉGRITÉ DU LOGICIEL D'APPAREILLAGE INSTALLÉ

SonovaVerify est intégré au logiciel d'appareillage et s'exécute à chaque lancement de l'application pour vérifier l'intégrité des fichiers de programme du logiciel d'appareillage. Les fichiers de programme sont signés numériquement à l'aide de pratiques normalisées du secteur et de certificats émis par une autorité de certification de confiance. Le logiciel avertit l'utilisateur via des messages d'avertissement si des fichiers de programme sont compromis.

8.4 VÉRIFICATION MANUELLE DE L'INTÉGRITÉ DU LOGICIEL D'APPAREILLAGE INSTALLÉ

Les utilisateurs peuvent effectuer les étapes suivantes pour vérifier l'intégrité et l'authenticité du logiciel d'appareillage installé à tout moment sans avoir besoin de lancer le logiciel d'appareillage :

1. Ouvrez l'Explorateur Windows et accédez au dossier exécutable du logiciel d'appareillage, généralement situé dans : C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Faites un clic droit sur SonovaVerify.exe et sélectionnez Propriétés dans le menu contextuel.
3. Sélectionnez l'onglet Signatures numériques.
4. Double-cliquez sur la signature SHA256 « Sonova AG ».
5. Vérifiez que les éléments de la signature sont valides, en particulier que le message « The digital signature is OK. » (La signature numérique est valide.) apparaît en haut et que le nom du signataire et l'heure de signature correspondent à l'image suivante :



1. Fermez les boîtes de dialogue contextuelles et double-cliquez sur SonovaVerify.exe.
2. Vérifiez que « NO ERRORS DETECTED » (AUCUNE ERREUR DÉTECTÉE) s'affiche comme indiqué dans l'image suivante :

L'image montre que SonovaVerify a authentifié et vérifié les signatures numériques de tous les fichiers de programme installés. Cela permet de vérifier que le logiciel d'appareillage n'a pas été altéré, corrompu ou compromis d'une autre manière. SonovaVerify affichera des avertissements ou des messages d'erreur si des fichiers ou des dossiers sont manquants ou si des fichiers ou des dossiers inattendus ont été ajoutés au dossier des fichiers du programme.

9. CORRECTIFS ET MISES À JOUR LOGICIELS

Les mises à jour automatiques ne sont pas prises en charge.

10. GESTION DES DONNÉES

10.1 BASE DE DONNÉES

Le logiciel d'appareillage utilise une base de données transactionnelle pour stocker les données des patients et un ensemble de bases de données d'informations qui fournissent les configurations de métadonnées requises par l'application.

Consultez la section 3. Diagrammes de réseau et de contexte – Artéfacts de déploiement pour obtenir une liste détaillée de toutes les bases de données déployées par le logiciel d'appareillage.

Lorsque le logiciel d'appareillage est installé en tant qu'application autonome, la base de données des patients est interne au logiciel d'appareillage. La base de données des patients, stockée dans le fichier PatientDatabase.sqlite, se trouve sur la même machine que le logiciel d'appareillage et fournit le stockage des données des patients. Pour sauvegarder les données d'application lorsque Target CI est déployé en tant qu'application autonome, créez une copie de sauvegarde de l'intégralité du dossier situé à l'emplacement %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Protégez les sauvegardes de données non seulement contre la perte de données, mais également contre le vol. Lorsque le logiciel d'appareillage est installé en tant que module Noah, les données des patients sont stockées dans la base de données fournie par le système Noah. La base de données Noah peut être configurée pour l'accès au réseau. La base de données Noah peut également être configurée pour un accès hors réseau et installée sur le même PC que le logiciel d'appareillage. Configurez le chiffrement de la base de données Noah pour protéger les données (reportez-vous à la documentation HIMSA).

Pour le mode de déploiement distribué de Noah, reportez-vous au lien suivant pour obtenir des instructions sur la sauvegarde et la restauration de la base de données des patients Noah :

https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/

10.2 MIGRATION DES DONNÉES

Le logiciel d'appareillage permet aux utilisateurs de migrer les dossiers des patients depuis le logiciel d'appareillage précédent d'AB, SoundWave 3.2. Les dossiers des patients doivent être accessibles depuis une installation SoundWave 3.2 sur le même ordinateur que Target CI afin d'être migrés.

10.3 CONFIGURATIONS DES APPAREILS AUDITIFS

Le logiciel d'appareillage permet d'exporter et d'importer la configuration et les paramètres de l'appareil.

10.4 ÉLIMINATION DES DONNÉES

Les instructions relatives à l'élimination des données se trouvent dans les instructions d'utilisation (IFU) ou sur le site suivant pour les déploiements de Noah : https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

11. ENVIRONNEMENT DE SÉCURITÉ – RESPONSABILITÉ PARTAGÉE

Le logiciel d'appareillage a été conçu pour une utilisation prévue dans laquelle la gestion des risques de cybersécurité est considérée comme une responsabilité partagée entre les parties prenantes de l'ensemble de l'écosystème des soins auditifs, qui incluent, sans s'y limiter, les utilisateurs d'appareils auditifs, les parents ou tuteurs légaux d'enfants qui sont des utilisateurs d'appareils auditifs, les audioprothésistes, les administrateurs informatiques, les établissements et prestataires de soins auditifs, les fournisseurs d'appareils auditifs et d'équipements de programmation.

Voici une liste de recommandations de bonnes pratiques courantes et de contrôles de sécurité pour l'environnement d'appareillage dans lequel le logiciel d'appareillage sera utilisé :

Niveau du système d'exploitation

- Appliquez des contrôles d'accès au niveau du système d'exploitation, par exemple :
  - Supprimez les comptes invités
  - Activez la connexion utilisateur Windows
  - Maintenez une liste d'opérateurs autorisés pour contrôler l'accès au système
  - Définissez des utilisateurs et des rôles personnalisés
  - Appliquez des exigences de mots de passe forts et gardez les informations d'identification secrètes
- Appliquez les contrôles d'audit au niveau du système d'exploitation
- Maintenez le système d'exploitation à jour
- Maintenez la version du logiciel d'appareillage installée à jour
- Activez la protection antivirus et contre les logiciels malveillants à jour
- Activez la liste blanche des applications

Protection des données

- Chiffrez les données des patients à l'aide d'outils ou de contrôles tiers au niveau du système d'exploitation, par exemple en utilisant le chiffrement de disque (par exemple, la fonctionnalité gratuite Microsoft BitLocker) pour protéger toutes les données. Pour les déploiements de Noah, envisagez d'utiliser le chiffrement de la base de données Noah.
- Les supports externes contenant des données exportées à partir du logiciel d'appareillage, y compris les rapports et les journaux, doivent être sécurisés. Lorsqu'elles ne sont plus utilisées, les données doivent être effacées de manière sécurisée et/ou les supports doivent être supprimés de manière sécurisée.
- Utilisez des supports de stockage USB dotés de fonctionnalités de sécurité intégrées, comme des clés USB chiffrées avec clavier intégré.
- Assurez-vous de toujours protéger vos données :
  - Lors du transfert de données via des canaux non sécurisés, envoyez des données anonymes ou chiffrez-les.
  - Protégez les sauvegardes de données non seulement contre la perte de données, mais également contre le vol.
  - Supprimez toutes les données du support de données qui ne sont plus utilisées ou qui doivent être éliminées.
- Les utilisateurs doivent utiliser des procédures et des outils approuvés pour la suppression sécurisée des données stockées sur des supports amovibles, conformément aux réglementations et directives applicables en matière de traitement des informations des patients / informations personnelles identifiables (IPI) / informations de santé protégées (ISP).

Infrastructure informatique

Utilisez le logiciel d'appareillage dans un environnement réseau sécurisé protégé contre toute intrusion non autorisée. Il existe de nombreuses techniques efficaces pour isoler et protéger les systèmes d'informations médicales, notamment la mise en œuvre d'une protection par pare-feu, de zones démilitarisées (DMZ), de réseaux locaux virtuels (VLAN) et d'enclaves réseau. Maintenez une connexion réseau active pour recevoir les mises à jour du système d'exploitation.

Niveau physique

- Le poste de travail sur lequel le logiciel d'appareillage est installé doit être physiquement sécurisé de manière à ce qu'il ne soit pas accessible aux utilisateurs non autorisés.
- Assurez-vous que le personnel non autorisé ne manipule pas le système.
- L'accès aux imprimantes connectées au poste de travail doit être contrôlé.
- L'écran du poste de travail où le logiciel d'appareillage est installé doit être placé de manière à limiter la visibilité du contenu de l'écran à l'utilisateur uniquement.

Niveau organisationnel

- Seul le personnel professionnellement formé et entièrement qualifié est autorisé à utiliser le système. Avant d'autoriser quiconque à utiliser le système, il convient de vérifier que la personne a lu et compris parfaitement les instructions d'utilisation fournies avec le logiciel d'appareillage.
- Si vous remarquez une activité suspecte sur vos comptes du logiciel d'appareillage ou une opération inattendue, contactez Advanced Bionics. Reportez-vous à la section 2.1 pour plus d'informations.

Pour plus d'informations sur la responsabilité partagée et pour obtenir une liste plus détaillée des recommandations de bonnes pratiques et des contrôles de sécurité pour l'environnement d'appareillage où le logiciel d'appareillage sera utilisé pour être appliqué à différents niveaux, reportez-vous :

- au livre blanc de l'EHIMA « Best Practices for Secure Fitting of Hearing Devices », EHIMAWhitePaper

12. PROCESSUS DE FABRICATION ET DE DÉVELOPPEMENT DU LOGICIEL

La cybersécurité est prise en compte tout au long du processus de développement logiciel. Le logiciel d'appareillage est développé en conformité avec les normes CEI 62304 et CEI 82304.

Le logiciel d'appareillage est analysé pour détecter la présence de virus et de logiciels malveillants dans le cadre du processus de fabrication.

Les vulnérabilités des composants tiers répertoriés dans la base de données nationale des vulnérabilités (National Vulnerability Databse, NVD) du National Institute of Standards and Technology (NIST) sont évaluées et réduites pendant le processus de développement et surveillées une fois que le logiciel d'appareillage a été mis sur le marché.

13. COMPOSANTS LOGICIELS ET NOMENCLATURE

Le logiciel d'appareillage intègre certains composants logiciels commerciaux prêts à l'emploi.

Le tableau suivant énumère tous les SOUP (logiciels de provenance inconnue) distribués avec le logiciel d'appareillage.

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
ciAD Hearingloss Simulator	Bibliothèque de simulateurs de perte auditive pour lecteur multimédia	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	Le package Credential Management est un wrapper pour l'API de gestion des informations d'identification Windows.	iLya Lozovyy	1.0.2
CSharpAnalytics	Utilisé pour Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78
Destructurama.Attributed	Utilisé par les bibliothèques Nephele	Contributeurs de Serilog	3.0
DirectShow 2005	Permet d'accéder à la fonctionnalité DirectShow de Microsoft à partir des applications .NET.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	National Centre for Audiology, Canada	4.2
DSL5	DSL 5 Fitting formula library	National Centre for Audiology, Canada	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical reconditionné pour Sonova	GNOtometrics	2.0.1.9
IceLink	Utilisé pour l'intégration des conférences audio/vidéo WebRTC	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect et bibliothèque cliente OAuth 2.0 utilisée par le composant Kona.CommonServices.Authentication pour l'authentification OAuth 2.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Bibliothèque d'interfaces de communication intermodules Noah	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Utilisé par les bibliothèques provenant de Sonova pour communiquer avec les contributeurs	Contributeurs de LibGit2Sharp	0.26.1
Mapster	Utilisé pour mapper des objets dans le code	chaowlert,eric_swann	7.2.0.0
MathNet.Numerics	Utilisé pour les algorithmes de l'appareillage (chemin du signal, outil de correspondance de cible, etc.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael et contributeurs	4.11.0
Microsoft.Bcl.AsyncInterfaces	Fournit les interfaces IAsyncEnumerable<T> et IAsyncDisposable et les types d'assistance pour .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Utilisé par les bibliothèques provenant de Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Utilisé par les bibliothèques provenant de Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Microsoft.Identity.Client	La bibliothèque MSAL pour .NET fait partie de la plateforme d'identité Microsoft pour développeurs (anciennement Azure AD) v2.0. Elle permet d'acquérir des jetons de sécurité pour appeler des API protégées. Elle utilise les normes industrielles OAuth2 et OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Cache de jetons multiplateforme sécurisé pour les applications client publiques MSAL	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Inclut des types qui fournissent un support pour la création, la sérialisation et la validation des Web JSON Tokens. Utilisé par les composants qui communiquent avec les services dorsaux qui utilisent des Web JSON Tokens pour l'authentification.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	Dépendance de Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Dépendance du SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Utilisé pour l'outil de sauvegarde du FSW (sauvegardes automatisées)	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	Les comportements XAML sont un moyen simple à utiliser d'ajouter une interactivité commune et réutilisable à vos applications WPF avec un minimum de code.	xamlexperiencesteam, Microsoft	1.0.1
MS VC++ 2008 Redistribuable	Microsoft Visual C++ 2008 Redistribuable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistribuable	Microsoft Visual C++ 2010 Redistribuable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistribuable	Microsoft Visual C++ 2012 Redistribuable	Microsoft	11.0.61030.0
Microsoft Visual C++ 2017 Redistribuable (x86)	Microsoft Visual C++ 2017 Redistribuable	Microsoft	14.16.27024.1
MS-VisualC++ 7.1 runtime libraries	Bibliothèques d'exécution Microsoft Visual C++	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1 Fitting formula library	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting formula library	Australian Hearing	2.0.11
NAudio.dll	Utilisé pour régler les volumes et lire des fichiers sonores	Open Source	1.9
.NET Framework	Cadriciel d'exécution .NET Framework	Microsoft	4.8.3928.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Newtonsoft.Json	Utilisé pour la sérialisation et la désérialisation JSON	James Newton-King	12.0.3
Nibelung	Bibliothèques d'appareillage NoahLink Wireless	GN ReSound	1.3.16.1
Nlog	Il s'agit d'une dépendance de Nibelung.CPD (Noahlink Wireless) de HIMSA.	Kim Christensen	4.4.0
NoahLink	Pilote de périphérique d'appareillage NoahLink	HIMSA	1.55.6.166
Noahlink Wireless	Pilote de périphérique d'appareillage Noahlink Wireless	HIMSA	2.0.0.68
Otometrics.HiPro2	Bibliothèques de communication HiPro	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Couche d'abstraction d'Otometrics au-dessus de la bibliothèque d'interface de communication intermodules Noah	GN Otometrics	1.0.0.10
PDFium.Net.SDK	La bibliothèque PDF C# permettant de créer et de modifier des documents PDF dans les applications .Net.	Patagames.com	4.54.2704.0
Polly	Bibliothèque qui permet aux développeurs d'exprimer des politiques de résilience et de gestion des fautes transitoires, telles que Retry, Circuit Breaker, Bulkhead Isolation et Fallback, de manière fluide et thread-safe	App vNext	7.2.1
Polly.Extensions.Http	Bibliothèque contenant des méthodes pratiques et avisées pour configurer les politiques Polly afin de gérer les fautes transitoires typiques des appels via HttpClient	App vNext	3.0
Polly.Contrib.WaitAndRetry	Bibliothèque pour Polly contenant des méthodes d'aide pour une variété de stratégies d'attente et de nouvelle tentative	Grant Dickinson, App vNext	1.1.1
Portable.BouncyCastle	Il s'agit d'une dépendance de Nibelung.CPD (Noahlink Wireless) de HIMSA.	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Cadre de sérialisation utilisé pour le blob RC	Open Source	2.0.0.668
Serilog	Composant de journalisation utilisé pour l'ensemble de l'application Chinook	Contributeurs de Serilog	2.10.0
Serilog.Enrichers.Thread	Enrichit les événements Serilog avec les propriétés du thread courant.	Contributeurs de Serilog	3.1
Serilog.Expressions	Filtrage d'événements basés sur des expressions pour Serilog	Contributeurs de Serilog	2.0
Serilog.Sinks.Console	Récepteur Serilog qui écrit les événements du journal dans la console/le terminal	Contributeurs de Serilog	4.0.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Serilog.Sinks.Debug	Récepteur Serilog qui écrit les événements du journal dans la fenêtre de sortie de débogage	Contributeurs de Serilog	2.0
Serilog.Sinks.File	Écrit les événements Serilog dans des fichiers texte au format brut ou JSON.	Contributeurs de Serilog	4.1
Serilog.Sinks.Trace	Récepteur de trace de diagnostic pour Serilog	Contributeurs de Serilog	2.1
Serilog.Settings.AppSettings	Configuration XML Prise en charge de (System.Configuration <appSettings>) pour Serilog	Contributeurs de Serilog	2.2.2
Security.Cryptography	Extensions des API de sécurité fournies avec .NET Framework	Microsoft	1.7.2
SharpBITS API	SharpBITS.NET est un wrapper .NET de l'API BITS et une petite application d'interface utilisateur Windows pour un accès plus facile aux téléchargements et téléversements avec BITS.	perpetualKid	2.1.0.0
SharpZipLib	#ziplib (SharpZipLib, anciennement NzipLib) est une bibliothèque Zip, Gzip, Tar et Bzip2 entièrement écrite en C# pour la plateforme .NET. Cette bibliothèque fournit des fonctionnalités de compression (compression, décompression, compression de flux, etc.). Nous l'utilisons dans l'application de mise à jour du micrologiciel.	Open Source	1.1.0.145
Superpower	Bibliothèque de combinateurs d'analyseurs pour C#	Datalust, contributeurs de Superpower, contributeurs de Sprache	2.3
SQLite.Interop	SQLite est une bibliothèque logicielle qui fournit un système de gestion de base de données relationnelle. Le « lite » dans SQLite signifie « léger » en matière de configuration, d'administration de base de données et de ressources requises. SQLite présente les fonctionnalités notables suivantes : autonome, sans serveur, sans configuration et transactionnel. Il s'agit d'une base de données (SQLite 3.32.1) permettant de stocker des informations sur le patient (en mode autonome), nos ressources de catalogue de produits et les métadonnées pour l'appareillage, les accessoires et les appareils auditifs.	Équipe de développement SQLite	1.0.113
System.Buffers	Fournit un regroupement de ressources de tout type pour les applications critiques en matière de performances qui affectent et désaffectent fréquemment des objets.	23rogramma,dotnetframework	4.5.1
System.Collections.Immutable	Utilisé par les bibliothèques provenant de Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.ComponentModel. Annotations	Fournit des attributs utilisés pour définir les métadonnées des objets utilisés comme sources de données.	23rogramma,dotnetframe work	4.7
System.Configuration.Configuration Manager	Fournit des types qui prennent en charge l'utilisation de fichiers de configuration.	Microsoft	5.0
System.Data.SQLite.Core	Utilisé par les bibliothèques provenant de Sonova.HardwareAbstraction. Palio.Trafo	Équipe de développement SQLite	1.0.113.7
System.Drawing.Common	Donne accès aux fonctionnalités graphiques de GDI+.	Microsoft	5.0.1
System.IdentityModel.Tokens.Jwt	Inclut des types qui fournissent une prise en charge pour la création, la sérialisation et la validation des Web JSON Tokens. Utilisé par les composants qui communiquent avec les services dorsaux qui utilisent des Web JSON Tokens pour l'authentification.	Microsoft	6.8.0
System.IO.Abstractions	Ensemble d'abstractions pour aider à rendre les interactions du système de fichiers testables	Tatham Oddie & friends	12.0.10
System.Numerics.Vectors	Fournit des types numériques accélérés par le matériel, adaptés aux applications de traitement et graphiques hautes performances.	24rogramma,dotn etfra me work	4.5
System.Memory	Fournit des types pour une représentation et un regroupement efficaces des segments de mémoire gérée, de pile et native et des séquences de ces segments, ainsi que des primitives pour analyser et formater le texte codé en UTF-8 stocké dans ces segments de mémoire.	24rogramma,dotn etfra me work	4.5.4
System.Reactive.Core	Extensions réactives (Rx) pour .NET	.NET Foundation	3.1.1
System.Reactive. Interfaces	Extensions réactives (Rx) pour .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Extensions réactives (Rx) pour .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Extensions réactives (Rx) pour .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Extensions réactives (Rx) pour .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Fournit une classe pour créer dynamiquement des types de proxy qui implémentent une interface spécifiée et dérivent d'un type DispatchProxy spécifié. Les invocations de méthode sur l'instance de proxy générée sont envoyées à ce type de base DispatchProxy.	Microsoft	4.7.1

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.Reflection.Metadata	Cet ensemble fournit un lecteur et un rédacteur de métadonnées .NET (ECMA-335) de bas niveau. Il est conçu pour les performances et constitue le choix idéal pour créer des bibliothèques de niveau supérieur qui visent à fournir leur propre modèle d'objet, comme des compilateurs.	Microsoft	5.0
System.Runtime.CompilerServices.Unsafe	Fournit la classe System.Runtime.CompilerServices.Unsafe, qui fournit des fonctionnalités génériques de bas niveau pour la manipulation de pointeurs.	24rogramma, dotnetframework	5.0
System.Security.AccessControl	Fournit des classes de base qui permettent de gérer les listes de contrôle d'accès et d'audit sur les objets sécurisables.	Microsoft	5.0
System.Security.Permissions	Fournit des types prenant en charge la sécurité d'accès au code (CAS).	Microsoft	5.0
System.Security.Principal.Windows	Fournit des classes permettant de récupérer l'utilisateur Windows actuel et d'interagir avec les utilisateurs et les groupes Windows.	Microsoft	5.0
System.Text.Encoding.CodePages	Fournit une prise en charge des codages basés sur les pages de codes, notamment Windows-1252, Shift-JIS et GB2312.	Microsoft	5.0
System.Text.Encodings.Web	Fournit des types pour l'encodage et l'échappement des chaînes à utiliser en JavaScript, en langage hypertexte (HTML) et dans les URL. Est une dépendance du SOUP IdentityModel	24rogramma,dotn etfra me work	5.0
System.Text.Json	Fournit des types hautes performances et à faible allocation qui sérialisent les objets en texte JSON (JavaScript Object Notation) et désérialisent le texte JSON en objets, avec prise en charge UTF-8 intégrée. Fournit également des types pour lire et écrire du texte JSON encodé en UTF-8 et pour créer un DOM (Document Object Model) en mémoire, en lecture seule, pour un accès aléatoire aux éléments JSON dans une vue structurée des données.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Fournit des types supplémentaires qui simplifient le travail d'écriture de code concurrent et asynchrone.	25rogramma,dotnetfra mework	4.5.4
System.ValueTuple	Fournit les structures System.ValueTuple, qui implémentent les types sous-jacents des tuples dans C# et Visual Basic. Ajoute la prise en charge des tuples de valeur, car ils ne sont inclus que dans les versions ultérieures de .NET Framework.	25rogramma,dotnetfra mework	4.5.0
Thrift	Utilisé pour la définition du protocole de liaison à distance	Apache	0.13.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Unity	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	5.8.13
WAP BT Dongle Driver	Pilote de dongle WAP BT (dongue d'appareillage)	iAnywhere Solutions	3.0.0.6095
WebSync	Utilisé pour l'intégration du canal de données d'appareillage	FM (Frozen Mountain)	4.9.32.0
Xps to Pdf render (NiXPS)	Convertit 25 fichiers XPS de manière programmatique en PDF ; utilisé dans les rapports d'application d'appareillage.	NiXPS	2.6.7.0

14. RÉFÉRENCES

Titre	Site Web
Instructions d'utilisation (électroniques)	https://ifu.advancedbionics.com/
Politique de confidentialité mondiale d'Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Backing up and restoring the data in your Noah database	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Noah System Database Capacity has been Reached.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
Ports et URL utilisés par TeamViewer	https://www.teamviewer.com/fr/global/support/knowledge-base/teamviewer-remote/troubleshooting/ports-used-by-teamviewer/?
BCP 195	https://www.rfc-editor.org/info/bcp195
Documentation sur la sécurité du serveur LiveSwitch	https://developer.liveswitch.io/liveswitch-server/server/security.html
Best Practices for Secure Fitting of Hearing Devices EHIMA whitepaper	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA Cybersecurity-FSW-Security-Whitepaper v1-Sep2021 .pdf

CE 0123

Advanced Bionics LLC
28515 Westinghouse Place
Valencia, CA 91355, United States
T : +1.661.362.1400

info.us@advancedbionics.com

EU REP Advanced Bionics GmbH
Feodor-Lynen-Strasse 35
D-30625 Hanovre

info.switzerland@advancedbionics.com

Pour plus d'informations sur les autres filiales AB existantes, consultez le site *advancedbionics.com/contact*

AB – Une marque Sonova

Veuillez contacter votre représentant AB pour vérifier l'autorisation réglementaire et la disponibilité dans votre région.

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S396-04 Rev A 2025-09-15